Week 3

CIA important concept in Cybersecurity.

Confidentiality. →

- is used to prevent any disclosure of data without prior authorization by the owner
- we can force confidentiality with encryption.
- Elements such as authentication, access controls, physical security and permissions are normally used to enforce confidentiality
-

Integrity

→ Normally implemented to verify and validate if the information that we sent or received has not been modified by an unauthorized person of the system

Online Hash generator. → we can implement technical controls such as algorithms or hashes (MD5, SHA1, etc).

→

Availability → The basic principle of this term is to be sure that the information and data

is always available when needed.

Technical Implementation

- RAIDS
- Clustery
- ISP Redundy
- Backups.

Non- Repudiation

Valid proof of the identity of the data sender & receiver.

Technical implementation:
- Digital Signatures
- Logs

Access Management.

Access Criteria
- Groups
- Time Frame and Specific dates
- Physical Location
- Transaction type
- "need to know" concept
- Single-Sign-On (SSO)

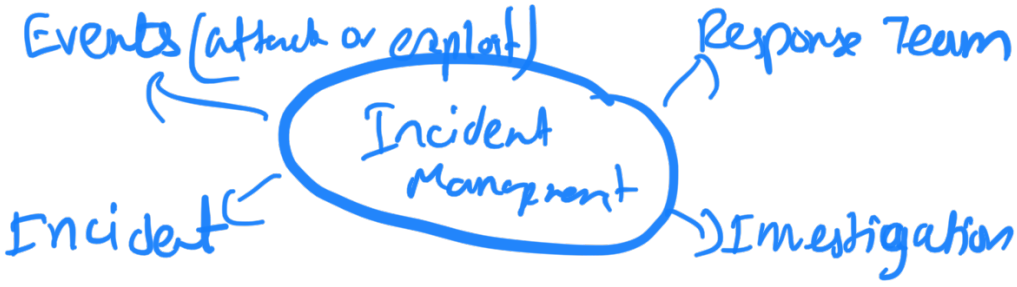
Authentication.
- Identity proof
- Kerberos (SSO)
- Mutual Authentication

-SMS-(MTP-v2

→ SPP's vs DACL's
- Security FP (Active Directory)
- Discretionary Access Control List.

Incident Response

→ Incident management involves the monitoring and detection of security events on a computer or a computer network and the execution of proper responses to those events. Most the info security or the incident management team will regularly check and monitor the security events occurring on a computer on in our network.



Key Concepts.

E-Discovery
Automated Systems → SIEM, SOA, UBA, AI
BCP & Disaster Recovery
Post-Incidented

Data Analysis

Incident Response Process

Phase 1 Prepare.
↳ conduct a critically assessment Bx

organization
↳ Carry out a cyber security threat analysis supported by realistic scenarios and rehearsals
↳ Considers the implications of people, process and technology and their
↳ Create appropriate control framework
↳ Review your state of readiness in Cyber Security Incident Response.

Phase 2 Respond.

↳ Identify cyber security incident
↳ Define objectives and investigate situation
↳ Take appropriate action
↳ Recover system, data and connections.

Phase 3 Follow up

↳ Investigate information more thoroughly
↳ Report to relevant Stakeholders
↳ Carry out a post incident review
↳ Communicate and build on lessons learned
↳ Update key information, controls and processes
↳ Perform trend analysis.

Data Breach Avoidance
↳ Incident Response team
→ Extensive use of encryption
→ Employee training.

Framework and their Purpose.

Best Practices, baselines and Frameworks

→ used to improve the controls, methodology and governance for the IT departments or the global behavior of the organization.

→ seeks to improve performance, controls, and metrics

→ Helps to translate the business needs into technical or operational needs.

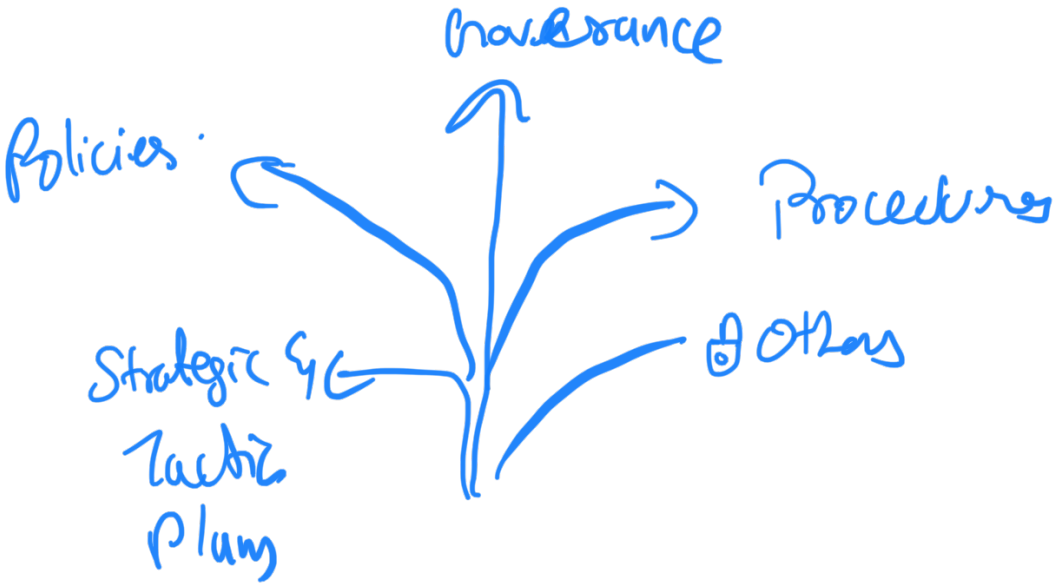
Normative and Compliance

→ Rules to follow for a specific industry
→ Enforcement for the government, industry or clients
→ Event if the company or the organization do not want to implement those controls for compliance.

Best Practice.

→ COBIT — Project Management methodologies
→ ITIL — Industry Best practices
→ ISO, — Developer recommendations
→ COSO — others.

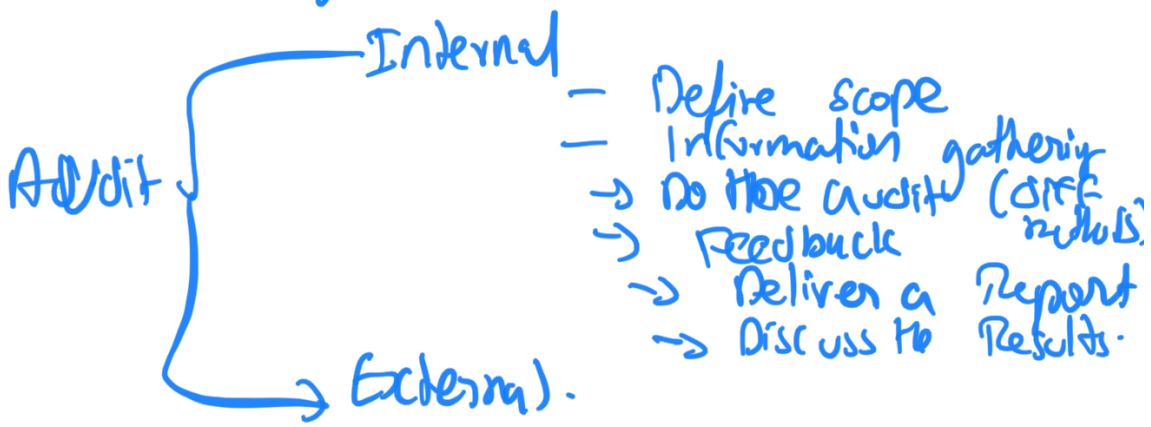
IT Governance Process.



Cybersecurity process Compliance and Audit

- SOX
- HIPPA
- GLBA
- PCI/DSS

Audits from SANS.org



The OCTAVE method.

Phase 1 → Organizational View
Phase 2 → Technological View
Phase 3 → Risk Analysis

PenTest Process and Mile 2 CPTE Training.

PenTest → Ethical Hacking.
a method for evaluating computer & network security simulating an attack on a computer systems or network from external or internal threats.

OWASP Framework -

A1 - Injection
A2 - Broken Authentication and sessi. manage
A3 → Cross-Site Scripting.
A4 → Insecure Direct Object References.

A5 → Security Misconfiguration
A6 → Sensitive Data Exposure

A7 → Missing Function Level Acces Control

A8 → Cross-Site Request Forgery

A9 → Using Known Vulnerable Components

A10 → Unvalidated Redirects and Forwards.